

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TENNESSEE
AT CHATTANOOGA

IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED WITH THE
CELLULAR DEVICE ASSIGNED CALL
NUMBER (404) 983-4056 (Target Telephone
1) and (504) 390-6445 (Target Telephone 2)
THAT IS STORED AT PREMISES
CONTROLLED BY AT&T WIRELESS

Case No. 1:19-mj- 77

Filed Under Seal

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Matthew Hennessee, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with a certain cellular telephone assigned call number (404) 983-4056 (Target Telephone 1 “TT-1”) and (504) 390-6445 (Target Telephone 2 (“TT-2”)), (the “Target Cellular Devices”), that is stored at premises controlled by AT&T WIRELESS, a wireless telephone service provider headquartered in Dallas, Texas. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. § 2703(c)(1)(A) to require AT&T to disclose to the government copies of the information further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review the information to locate items described in Section II of Attachment B.

2. I am a Task Force Officer with the Federal Bureau of Investigation (“FBI”), and have been since May 2001. I have also been a police officer with the Chattanooga Police Department (“CPD”) in Chattanooga, Tennessee since for approximately 24 years. During my

tenure as an investigator assigned to narcotics and violent crime investigations, I have gained a working knowledge of narcotics trafficking methods and techniques as well as violent crimes, including armed bank robbery, kidnapping, firearms use, etc. I have been training to conduct federal criminal investigations, particularly with respect to violent crime, locating and acquiring evidence of criminal activity, including cellular telephones, and seizing evidence and assets related to/derived from such criminal activity.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrants and does not set forth all of my knowledge about this matter.

4. Based on the facts set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. § 1201 (Kidnapping) and 18 U.S.C. § 2113(a) (Bank Robbery) have been committed by DANIEL CLAYTON BRYANT. There is also probable cause to search the information described in Attachment A for evidence of these crimes as further described in Attachment B.

PROBABLE CAUSE

5. The United States, including the FBI, is conducting a criminal investigation of DANIEL CLAYTON BRYANT regarding possible violations of 18 U.S.C. §§ 1201 and 2113(a).

- a. On April 4, 2019, at approximately 1253 hours, officers with the Chattanooga Police Department responded to the Bank of America located at 3620 Tennessee Avenue, Chattanooga, Tennessee, in response to a report of a kidnapping. Once on-scene, officers made contact with the victim. The victim told officers that he had been taken against his will and forced to withdraw thousands of dollars from his bank account, and provided documentary evidence showing the transaction history proving the amount of money withdrawn. The CPD violent crimes unit responded and further interviewed the victim.
- b. The victim stated that on Monday, April 1, 2019, at approximately 1200 hours, he

dropped his pickup truck at Mountain View Chevrolet to have the vehicle serviced. The victim had recently purchased the truck at Mountain View Chevrolet after receiving a substantial financial settlement resulting from severe on-the-job injuries that caused him to have one leg amputated and left him paralyzed on one side. The victim was offered a ride home by a Mountain View salesman identified by the victim as DANIEL CLAYTON BRYANT.

- c. After the victim got into BRYANT's vehicle, BRYANT transported the victim against his will to the Bank of America branch located on Gunbarrel Road in Chattanooga, Tennessee. BRYANT threatened to kill the victim and his family if the victim did not withdraw money from the victim's account. Over the course of two days, between April 1 and April 3, 2019, BRYANT held the victim against his will and transported him to several bank branches in the Eastern District of Tennessee and elsewhere, forcing him to withdraw money from his account under fear of death. As a result of this threat, the victim did withdraw money from his accounts at the Bank of Tennessee, Gunbarrel Road bank branch, as well as other bank locations, all of which were then federally insured by the Federal Deposit Insurance Corporation ("FDIC"), totaling approximately \$199,000 in cash and cashier's checks made out to BRYANT.
- d. During the kidnapping, BRYANT took the victim across state lines to a hotel room in or near Atlanta, Georgia, where BRYANT took the victim's cell phone and credit cards, and forced the victim to smoke crack cocaine, before returning the victim to Mountain View Chevrolet on April 3, 2019.
- e. On April 5, 2019, the FBI obtained bank records from Pinnacle Bank, in Nashville, Tennessee, related to the deposit of cashier's checks drawn upon the victim's Bank of America account and deposited into the account of BRYANT. As a result of this inquiry, the FBI learned that on April 1, 2019, Bryant deposited \$23,000 into his Pinnacle Bank Account, which consisted of Bank of America Cashier's Check, No. 119200117771, issued from the Bank of America on Gunbarrel Road, Chattanooga, Tennessee, made out to BRYANT, in the amount of \$12,000.00 drawn from the victim's account, plus \$11,000 in cash. At the time he obtained the \$12,000 cashier's check, BRYANT also forced the victim to withdraw \$12,000 in cash from the victim's Bank of America account. On April 3, 2019, BRYANT deposited a Bank of America Cashier's Check, No. 1271921701, issued from the Bank of America at Arbor Place Mall in Douglasville, Georgia, made out to BRYANT, in the amount of \$175,000 drawn from the victim's account into BRYANT's Pinnacle Bank Account.
- f. The FBI has been actively looking for BRYANT since April 4, 2019, the date the kidnapping report was taken, but has been unable to locate him as of April 8, 2019. The FBI has learned that BRYANT has been and is currently using two AT&T cellular telephones: (404) 983-4056 and (504) 390-6445 (the Target Cellular Devices), and has been using each of these phones to make numerous calls, including calling law enforcement on April 4, 2019, contacting co-workers at Mountain View Chevrolet, and calling other witnesses. On April 8, 2019, the FBI confirmed with AT&T that both of the

Target Cellular Devices have been active during the period of the kidnapping and are still active. Investigators believe BRYANT had these phones in his possession during the period of the kidnapping.

- g. In the undersigned's experience, subscriber information, including toll data from numbers obtained from numbers captured by pen registers, trap and trace devices and cell site data has yielded information that is relevant and material to identifying the location of criminal during the commission of a crime and is particularly useful in tracking a criminal's behavior during a criminal episode that occurred across state lines. The undersigned submits that there is probable cause to believe that the suspect—DANIEL CLAYTON BRYANT—has committed violations of 18 U.S.C. §§ 1201 and 2113(a), and was using and in possession of the Target Cellular Devices during the commission of these offenses, and that there is probable cause to obtain the historical cell-site location information for the period of the initial kidnapping and BRYANT's subsequent evasion of arrest: April 1, 2019, through April 9, 2019.

6. In my training and experience, I have learned that AT&T Wireless is a company that provides cellular telephone access to the general public. I also know that providers of cellular telephone service have technical capabilities that allow them to collect and generate information about the locations of the cellular telephones to which they provide service, including cell-site data, also known as "tower/face information" or "cell tower/sector records." Cell-site data identifies the "cell towers" (i.e., antenna towers covering specific geographic areas) that received a radio signal from the cellular telephone and, in some cases, the "sector" (i.e., faces of the towers) to which the telephone connected. These towers are often a half-mile or more apart, even in urban areas, and can be 10 or more miles apart in rural areas. Furthermore, the tower closest to a wireless device does not necessarily serve every call made to or from that device. Accordingly, cell-site data provides an approximate location of the cellular telephone but is typically less precise than other types of location information, such as E-911 Phase II data or Global Positioning Device ("GPS") data.

7. Based on my training and experience, I know that AT&T Wireless can collect cell-site data about the TARGET CELLULAR DEVICES. I also know that wireless providers

such as AT&T Wireless typically collect and retain cell-site data pertaining to cellular phones to which they provide service in their normal course of business in order to use this information for various business-related purposes.

8. Based on my training and experience, I know that wireless providers such as AT&T typically collect and retain information about their subscribers in their normal course of business. This information can include basic personal information about the subscriber, such as name and address, and the method(s) of payment (such as credit card account number) provided by the subscriber to pay for wireless telephone service. I also know that wireless providers such as AT&T typically collect and retain information about their subscribers' use of the wireless service, such as records about calls or other communications sent or received by a particular phone and other transactional records, in their normal course of business. In my training and experience, this information may constitute evidence of the crimes under investigation because the information can be used to identify the TARGET CELLULAR DEVICES' user or users and may assist in the identification of co-conspirators and/or victims.

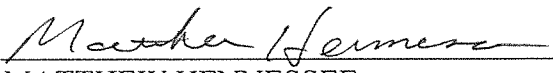
AUTHORIZATION REQUEST

9. Based on the foregoing, I request that the Court issue the proposed search warrant, pursuant to 18 U.S.C. § 2703(c) and Federal Rule of Criminal Procedure 41.

10. I further request that the Court direct AT&T Wireless to disclose to the government any information described in Section I of Attachment B that is within its possession, custody, or control. Because the warrant will be served on AT&T, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

11. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation, including by giving targets an opportunity to destroy or tamper with evidence, change patterns of behavior, notify confederates, and flee from prosecution.

Respectfully submitted,


MATTHEW HENNESSEE
TASK FORCE OFFICER
FEDERAL BUREAU OF INVESTIGATION

Subscribed and sworn to before me on April 9, 2019.


CHRISTOPHER H. STEGER
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to Be Searched

This warrant applies to records and information associated with the cellular telephone assigned call number (404) 983-4056 (Target Telephone 1) and (504) 390-6445 (Target Telephone 2), that are stored at premises controlled by AT&T Wireless ("the Provider").

ATTACHMENT B

Particular Things to be Seized

I. Information to be Disclosed by the Provider

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, including any information that has been deleted but is still available to the Provider or that has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose to the government the following information pertaining to the Account listed in Attachment A for the time period April 1, 2019 through April 9, 2019:

- a. The following information about the customers or subscribers of the Account:
 - i. Names (including subscriber names, user names, and screen names);
 - ii. Addresses (including mailing addresses, residential addresses, business addresses, and e-mail addresses);
 - iii. Local and long distance telephone connection records;
 - iv. Records of session times and durations, and the temporarily assigned network addresses (such as Internet Protocol ("IP") addresses) associated with those sessions;
 - v. Length of service (including start date) and types of service utilized;
 - vi. Telephone or instrument numbers (including MAC addresses, Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifier ("MEID"); Mobile Identification Number ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Number ("MSISDN"); International Mobile Subscriber Identity Identifiers ("IMSI"), or International Mobile Equipment Identities ("IMEI");
 - vii. Other subscriber numbers or identities (including the registration Internet Protocol ("IP") address); and

- viii. Means and source of payment for such service (including any credit card or bank account number) and billing records.
- b. All records and other information (not including the contents of communications) relating to wire and electronic communications sent or received by the Account, including:
 - i. the date and time of the communication, the method of the communication, and the source and destination of the communication (such as the source and destination telephone numbers (call detail records), email addresses, and IP addresses); and
 - ii. information regarding the cell tower and antenna face (also known as “sectors”) through which the communications were sent and received.

II. Information to be Seized by the Government

All information described above in Section I that constitutes evidence of violations of 18 U.S.C. § 1201 (Kidnapping), 18 U.S.C. § 2113(a) (Bank Robbery) and evading law enforcement involving DANIEL CLAYTON BRYANT during the period April 1 through April 3, 2019.

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the records produced by the Provider in order to locate the things particularly described in this Warrant.